How Do You Overcome and Fight Back Against Cyber Attacks

How do you overcome a challenge like cyber security? It's a question that continues to confuse and frustrate businesses of all shapes and sizes, and is more pertinent today than ever before. Almost every day we seem to read stories of those who have suffered the consequences of not having sufficient measures in place to protect themselves — you don't need to cast your mind back far to remember what happened to the payday loan company Wonga.

As cyber attacks continue to grow in both their rate and their sophistication, businesses are left with no option but to sit up and pay attention to what has become a serious issue. It wasn't too long ago when businesses thought they could get away with taking a reactive approach — many simply would not consider the threat of cyber attacks until they were faced with one, at which point they would try (and often fail) to deal with it effectively. But businesses cannot afford to do this anymore. Instead, they need to take a proactive approach that includes preparations and measures to mitigate risks and protect all valuable data and assets.

However, depending on the size and nature of the business, adopting this proactive stance is often easier said than it is done. The biggest issue for most businesses is convincing the senior leadership teams that cyber security is something worth actively investing in. Originally, back when businesses were fighting online attacks reactively, cyber security used to be exclusively dealt with by IT departments. But the issue is much larger than it used to be and now requires company-wide participation. What's more, even with the backing of senior management, it can be hard for businesses to know where to begin in their cyber security journey.

The solution to effectively fight back against cyber attacks is through the implementation of a cyber security strategy. This is a comprehensive set of best practices that covers every eventuality and is distributed to all employees, raising awareness of the issue and making sure everyone knows exactly what to do in the event of an attack.

However, these are not simply copy and paste jobs: each strategy needs to be tailored to the specific nature and requirements of each business. If daily responsibilities regularly include the handling of personal data, for example, then the strategy should outline any additional risks this poses and suggest effective ways of mitigation. When an attack does take place, the strategy should be able to help define the attack, identify what's been affected and help make the recovery process much smoother. It shouldn't just be left on a shelf to be forgotten about, either; it should be regularly referred to and updated to ensure everyone is on the same page.

When devising these cyber security strategies, there are several factors that should also be considered to help make them more effective.

Firstly, businesses should think about how many employees are regularly working from home or outside of the office and how this could present security risks. These individuals might be working with confidential data while sat in a public space, or they might be saving documents directly to their devices without backing them up or storing on an internal company network. This means that if the data is compromised, it's gone forever.

In fact, businesses need to check that they are regularly backing up all areas of the network that are used to save or edit work. While it's easy to lighten the workload by only backing up the folders that are used most frequently, a comprehensive backup routine will prevent any serious cyber attack repercussions later down the line.

One small step that can make a huge difference is introducing a password policy. We've all been warned of the dangers of weak passwords before, but it's something that continues to cause trouble for businesses, especially when you consider how many people use the same password for multiple accounts. Making sure all employees are using strong passwords should not be taken lightly, and this applies to any device that is connected to the internet, including phones, printers, IoT (Internet of Things) devices and more.

Finally, all businesses should identify any vulnerabilities that exist within their IT infrastructure. Many companies are still using old, outdated technology as part of their IT systems, and much of this can simply be exploited by cyber criminals looking for an easy target. As a result, this technology should be updated wherever possible to maximise defences, or failing that there should be extra preventative measures in place to deter any hopeful attackers.

While it's ultimately difficult to completely stop cyber criminals from trying to wreak havoc, it is completely within the power of businesses to reduce the overall impact of the cyber criminals' actions through proactive efforts.

Link to the original article:
https://www.comparethecloud.net/articles/how-do-you-overcome-and-fight-back-against-cyber-attacks/